

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)INFORMATION ASSOCIATED WITH (513) 302-4488, IMEI:  
357340094884330 THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE, INC.

Case No.

1:19MJ-447

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

21 U.S.C. 841(a)(1) and 846 Conspiracy to Possess and Possession with Intent to Distribute Cocaine

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Mitchell S. Bedard, Special Agent, DEA

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/5/19

Judge's signature

City and state: Cincinnati, Ohio

Hon. Karen L. Litkovitz, U.S. Magistrate Judge

Printed name and title

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with **(513) 302-4488, IMEI: 357340094884330** (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”),

Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from May 1, 2019 through June 4, 2019, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account May 1, 2019 through June 4, 2019, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all



address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of the service of this warrant.

**II. Information to be seized by the government**

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations 21 U.S.C. § 841(a)(1) and 846 involving Damon BRIERS, and others during the period May 1, 2019 through June 4, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
(513) 302-4488, IMEI: 357340094884330  
THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE, INC.

Case No.

**19 MJ - 447**

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Mitchell S. Bedard, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent ("SA") of the Drug Enforcement Administration ("DEA") and have been so employed since November 2017. Prior to being employed with the DEA, I was employed by Butler County, Ohio as a probation officer for over four years. I graduated from the DEA Basic Agent Academy in May 2018. During the courses of my training, I received instruction in the investigation of offenses involving controlled substances. As a Special Agent of the DEA, my duties and responsibilities include conducting criminal investigations for violations of federal



law, particularly those found in Title 21 and Title 18 of the United States Code. As a DEA agent, I have participated in multiple criminal investigations seeking evidence of violations of the Federal Controlled Substances Act (Title 21 of the United States Code).

3. I am currently assigned to the Cincinnati Resident Office of the DEA. Prior to my assignment, I received specialized training from the DEA, including the 18-week Basic Agent Training course. Among other things, this training focused on: methods of unlawful drug trafficking; the identification of controlled substances; surveillance; undercover operations; confidential source management; the means by which drug traffickers derive, launder, and conceal their profits from drug trafficking; the use of assets to facilitate unlawful drug trafficking activity; and the law permitting the forfeiture to the United States of assets purchased with drug proceeds or assets used or intended to be used to facilitate the drug violations.

4. My knowledge of the matters contained in this affidavit is based upon my personal knowledge, information provided to me by other law enforcement officers/agents, and information provided to me by one or more Confidential Sources (CS) and/or Sources of Information (SOI). I have not included each and every fact of which I or other investigators are aware, as that is not the purpose of this Affidavit, as further described below.

5. Through my training and experience, I know that those involved in the illegal sale and distribution of narcotics often store in their cell phones and mobile devices, contact information for their associates so that they may stay in ready contact with their customers and source(s) of supply. Often the information stored in the contact list may be in the form of a code to conceal the true identity of the contact. I am also aware that drug traffickers often communicate with their customers, couriers, and/or associates through the use of cellular telephones or use of multiple telephones or other devices, to avoid detection by law enforcement.



6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 21 United States Code, Sections 841(a)(1) and 846 have been committed, are being committed, and will be committed by Damon BRIERS, and as-yet known and unknown individuals. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

#### **JURISDICTION**

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **PROBABLE CAUSE**

9. In May 2019, the Cincinnati Police Department received information from a confidential source (CS) regarding cocaine trafficker Damon BRIERS. The CS has been charged with drug trafficking offenses and is cooperating in exchange for consideration on these pending charges. Officers/agents have been able to independently corroborate information provided by the CS and therefore deem the CS reliable.

10. The CS stated BRIERS is actively trafficking cocaine in Cincinnati, Ohio. The CS stated Briers lives at a residence on Vine Street, in the neighborhood of Avondale, and drives a tan/brown conversion van. The CS stated BRIERS uses (513) 302-4488 (the **SUBJECT**

**TELEPHONE**) to communicate with customers regarding cocaine sales. Officers/agents are familiar with BRIERS from previous illegal drug trafficking investigations and showed the CS a recent Ohio Bureau of Motor Vehicles image of BRIERS. The CS positively identified the image as that of BRIERS.

11. Ohio BMV records indicated BRIERS listed his address as 3672 Vine Street, in the neighborhood of Avondale, and owns a tan/brown 2004 GMC Conversion Van, which I believe corroborates the information provided by the CS.

12. On May 12, 2019, at approximately 3:48PM, the CS conducted an unrecorded telephone call with BRIERS on the **SUBJECT TELEPHONE**. The CS reported controlling officers/agents the details of this conversation and officers/agents confirmed that this call took place by reviewing call records for the **SUBJECT TELEPHONE**. The CS stated BRIERS indicated his cocaine source of supply currently had kilogram quantities of cocaine available for sale at the rate of \$30,000 per kilogram.

13. At approximately 4:19 p.m., the CS received a text message, in the form of an iMessage, from BRIERS using the **SUBJECT TELEPHONE**. The text message stated "No break down." The CS sent a screenshot of this message to controlling officers/agents to document the conversation. The CS stated this text message indicated BRIER's cocaine source of supply did not want to sell less than kilogram quantities of cocaine to BRIERS.

14. On May 13, 2019, controlling officers/agents directed the CS to conduct a recorded telephone call to BRIERS on the **SUBJECT TELEPHONE**. During the call, BRIERS discussed the current availability of cocaine available for resale and purchase price for this cocaine. Controlling officers/agents were in close proximity to the CS during the call and were able to

monitor the call as it took place. Officers/agents subsequently confirmed that the CS called the **SUBJECT TELEPHONE** by reviewing call records.

15. Officers learned the **SUBJECT TELEPHONE** is subscribed to “Terri C Wallace,” to a device assigned International Mobile Equipment Identity (IMEI) 357340094884330. Officers are aware illegal drug traffickers regularly use cellular telephones subscribed in the name of others to thwart law enforcement identification efforts. The device assigned IMEI 357340094884330 is an Apple iPhone XR.

16. Based on the information in this affidavit, Affiant believes it reasonable to conclude that evidence of crime, and specifically of narcotics-related crimes, is likely to be found in the execution of the requested warrant.

#### **INFORMATION REGARDING APPLE ID AND iCloud<sup>1</sup>**

17. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

18. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

---

<sup>1</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.



- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.
- d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.
- e. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

19. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

20. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email

addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

21. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

22. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

23. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address



and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

24. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud Drive. Some

of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

25. Based on the information in this affidavit, Affiant believes it reasonable to conclude that evidence of crime, and specifically of narcotics-related crimes, is likely to be found in the execution of the requested warrant. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

26. Based on the communication between the user of the Apple ID and a Confidential Source, wherein the Apple ID user discusses cocaine prices and amounts available for sale, Affiant believes that the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

27. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. Furthermore, Affiant believes that information obtained from the Apple ID account could lead to investigators identifying associates, as-yet known and unknown, who are participating in a drug trafficking conspiracy. This "user attribution" evidence is analogous to the search for "indicia of occupancy"

while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

28. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. As mentioned in the affidavit, communication regarding illegal drug activity has been discussed, through cellular telephone calls, between the Apple ID user and a Confidential Source. However, a list of applications associated with the Apple ID may reveal other forms of communication that the user of the Apple ID engages in (i.e. WhatsApp, Snapchat, Viber). Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.



30. Based on the information in this affidavit, Affiant believes that between May 1, 2019 and June 4, 2019 evidence of a crime, and specifically of narcotics-related crimes, is likely to be found in execution of the warrant. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

31. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

32. Based on the forgoing, I request that the Court issue the proposed search warrant.

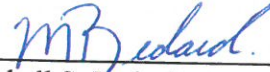
33. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

#### **REQUEST FOR SEALING**

34. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the

targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



\_\_\_\_\_  
Mitchell S. Bedard  
Special Agent  
Drug Enforcement Administration

Subscribed and sworn to before me on this 5 day of June 2019.



\_\_\_\_\_  
Hon. Karen L. Litkovitz  
United States Magistrate Judge

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with **(513) 302-4488, IMEI: 357340094884330** (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.



**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”),

Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from May 1, 2019 through June 4, 2019, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account May 1, 2019 through June 4, 2019, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all

address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of the service of this warrant.



**II. Information to be seized by the government**

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations 21 U.S.C. § 841(a)(1) and 846 involving Damon BRIERS, and others during the period May 1, 2019 through June 4, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple Inc. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple Inc., and they were made by Apple Inc. as a regular practice; and

b. such records were generated by Apple Inc.'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature